UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/623,830	07/21/2003	Astrid Elbe	S&ZIO020103	5757

7590 06/24/2004

LERNER AND GREENBERG, P. A.
P.O. BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
DO, CHAT C	

ART UNIT	PAPER NUMBER
2124	

DATE MAILED: 06/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/623,830	ELBE ET AL.	
	Examiner	Art Unit	
	Chat C. Do	2124	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/1/03; 10/27/03; 7/21/03*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-9* is/are rejected.

7)☒ Claim(s) *6 and 10-13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/1;10/27;7/21*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the limitations cited in claim 6 must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. The abstract of the disclosure is objected to because the abstract exceeds 150 words in length and is narrated in two paragraphs. Correction is required. See MPEP § 608.01(b).

4. The disclosure is objected to because of the following informalities:

The line "Fig. 2" in abstract page should be removed.

Throughout specification, there are a lot of words that clump together as seen in claim 1 line 31 "polynomialof".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2, 4-5, and 7-8 are rejected under 35 U.S.C. 103(a) as being obvious over Sedlak (U.S. 4,870,681) in view of Guido ("Should left shift test for overflow?").

Re claim 1, Sedlak discloses in Figures 4-6 method modular multiplying a multiplicand by multiplier using a modulus (abstract), multiplicand, multiplier and modulus being polynomials of a variable, with a cryptographic calculation, multiplicand, multiplier and modulus being parameters cryptographic calculation (col. 3 lines 21-47), method comprising the following steps: (a) performing a multiplication look-ahead method (Figure 4 and Figure 6(b)) to obtain a multiplication shift value (Sz), multiplication shift value being incremented at a power of multiplier (Sz = Sz +1 in Figure 4), which is not present in the multiplier polynomial; (b) multiplying (SHL Z, sz in Figure 6(b)) variable by an intermediate result polynomial to obtain shifted intermediate result polynomial (output of SHL Z, sz); (c) performing a reduction look-ahead method (Figure 5 and Figure 6(b)) to obtain reduction shift value (Sn), reduction

shift value (Sn) being equal to the difference the degree of shifted intermediate result polynomial and the degree of modulus polynomial (Sn = Sn + sz wherein Sn = -k in Figure 6(b)); (d) multiplying variable (SHL N, sn in Figure 6(b)) by modulus polynomial shifted modulus polynomial (output of SHL N, sn in Figure 6(b)); (e) summing shifted intermediate result polynomial and multiplicand and subtracting shifted modulus obtain a polynomial to obtain an updated intermediate result polynomial (Z := Z+a+P+b+N in Figure 6(b)); and (f) repeating (feedback when No to m = 0 and n =0 in Figure 6(b)) steps (a) to (e) until all the powers of multiplier have been processed, wherein in the repetition of step (a) to (e) in step (d) updated intermediate result polynomial of the previous step (e) is used as intermediate result polynomial, and in step (c) shifted polynomial of the previous step (d) is used as a modulus polynomial. Sedlak fails to disclose in steps (b) and (d) multiplying variable raised to the power multiplication shift value by an intermediate result polynomial; and multiplying variable raised to the power reduction shift value by modulus polynomial shifted modulus polynomial. However, Guido discloses a concept of multiplication in binary by shifting certain bit in a direction is equivalent to multiply a number base 2 raised to the power of shift value (page 1 6th paragraph e.g. X*8 or X* 2^8 is equivalent to shift left X by 3 positions). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a multiplication by raising to the power multiplication shift value in binary as disclose in Guido's discussion into Sedlak's invention because it would enable to simplify the circuitry.

Re claim 2, Sedlak fails to disclose multiplying in step (d) is carried out by shifting intermediate result polynomial by a number of digits equaling multiplication shift value, and wherein multiplying step (d) is carried out by shifting modulus polynomial by a number of digits equaling reduction shift value. However, Guido discloses a concept of multiplication in binary by shifting certain bit in a direction is equivalent to multiply a number base 2 raised to the power of shift value (page 1 6th paragraph e.g. X*8 or X* 2^8 is equivalent to shift left X by 3 positions). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a multiplication by raising to the power multiplication shift value in binary as disclose in Guido's discussion into Sedlak's invention because it would enable to simplify the circuitry.

Re claim 4, Sedlak further discloses a step of reduction look-ahead method (Figure 5 and Figure 6(b)) obtain a reduction shift value (b) comprises the following steps: determining an auxiliary shift value (b) so that the degree of modulus polynomial and the degree of updated intermediate result polynomial of the previous step multiplied by a variable which is raised to the power of auxiliary shift value are equal, and forming the difference of multiplication shift value and auxiliary shift value to obtain reduction shift value (mid portion of Figure 5).

Re claim 5, Sedlak further discloses in a step of performing multiplication look-ahead method (GEN_Mult_LA) and step of determining auxiliary shift value (GEN_MOD_LA) are carried out parallel to each other (Figure 6(b)).

Re claim 7, it is an apparatus claim of claim 1. Thus, claim 7 is also rejected under the same rationale in the rejection of rejected claim 1.

Re claim 8, it is an apparatus claim of claim 2. Thus, claim 8 is also rejected under the same rationale in the rejection of rejected claim 2.

7. Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being obvious over Sedlak (U.S. 4,870,681) in view of Guido ("Should left shift test for overflow?") and further in view of Dodson et al. (U.S. 5,251,164).

Re claim 3, Sedlak in view of Guido inherently discloses coefficients of polynomials can only take the values "0" or "1" (col. 1 lines 5-20), Sedlak in view of Guido fail to disclose summing and subtracting step carried out by bitwise XoRing intermediate result polynomial, multiplicand and shifted modulus polynomial. However, Dodson et al. disclose in Figures 7(b) and 8 a summing and subtracting is carried out by bitwise XoRing (806). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a summing and subtracting is carried out by bit-wise XORing as seen in Dodson et al.'s invention into Sedlak in view of Guido's invention because it would enable to reduce the circuitry and improve the system performance.

Re claim 9, it is an apparatus claim of claim 3. Thus, claim 9 is also rejected under the same rationale in the rejection of rejected claim 3.

Allowable Subject Matter

8. Claims 6 and 10-13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent No. 4,625,076 to Okamoto et al. disclose a signed document transmission system.

b. U.S. Patent No. 4,346,451 to Katayama discloses a dual module exponent transform type-high speed multiplication system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (703) 305-5655. The examiner can normally be reached on M => F from 7:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (703) 305-9662. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2124

June 3, 2004

KAKALI CHAKI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100